AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Shayne Tongbua, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I am a Special Agent of the Federal Bureau of Investigation (FBI) and have been employed with the FBI since 2009. In the course of my duties, I have investigated national security matters relating to economic espionage, international and domestic terrorism, weapons of mass destruction, and other federal criminal violations. I have acquired experience in investigating various violations of federal law through extensive training at the FBI Academy in Quantico, Virginia, and by conducting investigations in the field. During my career, I have participated in many criminal investigations as a case agent and/or in a subsidiary role and have participated in the execution of numerous federal search warrants.

2. I am currently assigned to the FBI New Hampshire (NH) Joint Terrorism Task Force (JTTF) and am currently the only certified FBI Bomb Technician in NH. As such, I routinely collaborate with federal, state, and local law enforcement counterparts in operations and investigations involving explosive devices and materials. I also participate in monthly training with other law enforcement public safety bomb technicians from across New England. I assist in quarterly certification training for K-9 explosive detection teams for local law enforcement agencies and at each airport in New Hampshire and Maine.

3. I have operated as a certified, public safety hazardous devices technician (bomb technician) since 2010. I have received additional training from the FBI Hazardous Devices School and gained extensive experience from advanced training and field operations. Prior to joining the FBI, I graduated from Naval School Explosive Ordnance Disposal (EOD) and served as a military bomb technician in the US Army from 2003-2009. I also gained additional

experience through advanced training and field operations, including an overseas deployment in support of Operation Iraqi Freedom (OIF III) and eventually becoming a certified EOD Team Leader.

4. I am a federal law enforcement officer of the United States within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), duly authorized to conduct investigations of and make arrests for violations of United States Code.

5. The probable cause set forth in this affidavit is based upon my personal knowledge and observations, experience and training, as well as through information derived from investigators of the Greenfield, NH Police Department (PD), the NH State Police, the NH Fire Marshal's Office, the FBI NH Offices, cooperating individuals, associated businesses, database queries, and review of electronic evidence.

6. Since the affidavit is being submitted for the limited purpose of establishing that probable cause exists to support the issuance of a search warrant, I have not included details about every aspect of the investigation. While this affidavit contains all the material information I am aware of that is pertinent to the requested search warrants, it does not set forth all of my knowledge about this matter.

7. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of the National Firearms Act, Title 26 U.S.C. § 5861(c), (f), and destruction of motor vehicles, Title 18 U.S.C. § 33, have been committed by Alexander ARSENAULT. There is also probable cause to search the location described in Attachment A for evidence of these crimes and contraband, as described in Attachment B.

PROBABLE CAUSE

8. On December 1, 2018, the Conway family, residents of Greenfield, NH, reported vandalism to their Jeep Grand Cherokee to Greenfield PD. Family members informed the responding officer that they heard a loud noise like an explosion around 6:30 AM that shook their home. They had received no prior threats and could not determine who might want to harm them or damage their property. They observed no suspicious activity the night before and observed no vehicles or people coming or going that night. The Conway family stated that their neighbor, ARSENAULT, had some previous "issues" with their boys riding their four wheeler.

9. Later on December 1, 2018, investigators from the NH State Police Bomb Squad and the NH Fire Marshal's Office responded to assist in conducting a post blast investigation at the request of Greenfield PD. Subsequent reports by both entities confirmed the event was consistent with an explosion. During the incident, photographs and physical evidence were obtained from a damaged Jeep Grand Cherokee on the property located at in Greenfield, NH. This property is adjacent to 21 School House Rd, ARSENAULT's residence. The physical evidence was transferred to FBI custody and sent to the FBI Laboratory in Quantico, VA for forensic analysis. Results are pending. A photograph of some of the damage is below:

10. On December 1, 2018, investigators interviewed ARSENAULT in his home. When asked if he knew anything about what happened to his neighbors, he stated he did not have any issues with his neighbors, but he gets annoyed when people ride by his house on the snowmobile trail. During the interview investigators observed several strips of gray duct tape on the walls of ARSENAULT's residence. The duct tape was consistent in appearance with pieces of duct tape recovered in and around the damaged vehicle at .

11. On December 20, 2018, a concerned individual[1] ("Individual") called the FBI Public Access Line and reported that ARSENAULT was acquiring Tannerite[2] and was interested in making miniature explosives. Specifically, Individual stated that ARSENAULT was building explosive targets out of Tannerite for target practice, and also sought to create miniature explosives. Individual also stated that ARSENAULT recently told Individual he wanted to acquire 100 cans of lighter fluid to make small explosions in his backyard and post videos of the explosions to YouTube. Individual indicated that ARSENAULT claimed to have researched the materials and acquired them from the websites tannerite.com and ammoniumnitrateforsale.com.

12. On January 4, 2019, investigators returned to ARSENAULT's residence to conduct a follow up interview. Investigators heard loud music coming from the residence, but ARSENAULT did not answer the door. Investigators observed and seized a piece of silver duct tape from the doorstep which closely resembled the tape recovered from the damaged Jeep Grand Cherokee, and was consistent with tape observed in ARSENAULT's home during his December 1, 2018 interview.

---

[1] Individual's identity is known to law enforcement and Individual is providing information as a concerned citizen. Individual's criminal history reveals no derogatory information.

[2] Tannerite is a binary exploding target package formed by combining separate oxidizer and catalyst compositions. Tannerite is a patented, legally obtainable product with legitimate uses intended for responsible consumers. Binary mixtures such as Tannerite and similar products comprised of ammonium nitrate and aluminum powder produce Ammonal when the two components are mixed. Ammonal is an explosive material as listed in the ATF 2018 Annual List of Explosive Materials and published in the Federal Register.

13. On January 9, 2019, Greenfield PD stated that they had received recent complaints of loud noises believed to be small explosions in the vicinity of ARSENAULT's residence. The noises were reported by multiple concerned citizens including one of the Conway's teenage sons. Greenfield PD also conveyed that ARSENAULT had made multiple complaints in the past regarding loud noises from vehicles revving the engines in front of his house, low-flying aircraft, nearby gunfire, as well as four wheeler and snowmobile traffic.

14. On January 18, 2019, Individual provided additional information indicating that ARSENAULT claimed to have purchased and resold Tannerite via eBay at least 15 times, and ARSENAULT used "lawaranda71" as his eBay username. Individual stated that ARSENAULT was interested in blowing up a shed on ARSENAULT's property.

15. Individual also provided law enforcement with two sets of digital photographs taken inside of ARSENAULT's home before December 20, 2018, showing at least two laptop computers present in the residence. One photograph depicts what appears to be an internet cable attached to a laptop by grey duct tape, while the laptop is powered on. A separate photograph shows ARSENAULT seated in front of, and apparently using, a laptop computer.

16. On January 23, 2019, open source research revealed that lawaranda71 had been an eBay member since September 25, 2017, and had received 122 feedback ratings/comments regarding various previous transactions. The research revealed three identified past transactions of explosive-related products, including Tannerite, Potassium Perchlorate, and Magnesium Metal Powder. The research also revealed thirteen current listings for explosive-related products, including Tannerite, Binary Targets, and Binary Target Fillers. At least four current listings indicated that the item location was in Greenfield, New Hampshire, United States. The "product

description" in multiple listings indicated that lawaranda71 had sold Tannerite to at least 15 customers.

17. Records received from a Grand Jury Subpoena to eBay revealed that lawaranda71 has purchased the following items between November 5 and November 13, 2018:

a. 3M Micropore Surgical Tape, 2 Inch X 10 Yards, 1530-2, NEW - 6 Count Box;

b. Touch Duct Tape Multi-use 2" x 45 Yard Grey Repair Wrapping Sealing Protecting; and

c. Diamond Strike on Box Matches Greenlight 2 Pack of 300 (600 Matches).

Each of these items is similar to items recovered from the damaged Jeep Grand Cherokee on December 1, 2018.

18. Records received from eBay confirm that lawaranda71 has sold Tannerite (ranging from 10 lbs to 50 lbs), potassium perchlorate, and magnesium metal powder from November 2018 through January of 2019.

19. eBay records also revealed the following name and contact information associated with User ID lawaranda71:

Alex Arsenault
21 School House Rd
Greenfield, NH 03047

20. Records received from ammoniumnitrateforsale.com confirm that ARSENAULT has purchased exploding target mix (ranging from 10 lbs to 50 lbs), similar to Tannerite, from December 2018 through February of 2019. The email address storeyfinder@gmail.com was provided for all orders under ARSENAULT's name.

21. ARSENAULT has not registered any firearms or destructive devices in the National Firearms Registration and Transfer Record.

22. ARSENAULT has a criminal history that includes charges for criminal mischief and simple assault with no convictions.

23. Based on my training and experience as a current FBI Bomb Technician and a former US Army EOD Technician, combined with the totality of the circumstances and extensive evidence revealed during the course of this investigation, there is probable cause to believe an improvised explosive device (IED) caused the vehicle destruction which occurred at in Greenfield, NH on December 1, 2018. There is also probable cause to believe Alexander ARSENAULT has procured and may still possess sufficient materials to construct one or more IEDs capable of such destruction. The proximity of ARSENAULT's residence, combined with previous statements expressing desire to create and use explosive charges and the acquisition of materials which could be used to construct IEDs, constitutes probable cause that ARSENAULT was responsible for the vehicle explosion.

24. In my training and experience, individuals who construct IEDs do so and store requisite materials in locations that are typically private and secure, such as a residence, garage or workshop. Doing so minimizes observation of these activities and risk of accidental initiation by others. These areas also typically contain tools and items useful in IED construction, but not always part of a device, such as scissors, pliers, wire cutters, screw drivers, glue, tape, etc. ARSENAULT is known to law enforcement to live alone and not to own a vehicle. Due to ARSENAULT's limited means of transportation and lack of access to other facilities, in conjunction with his expressed interest to create and use explosive charges and the acquisition of materials which could be used to construct IEDs, there is probable cause to believe

ARSENAULT has constructed previously and may continue to construct such devices on his property.

COMPUTERS, ELECTRONIC STORAGE AND FORENSIC ANALYSIS

25. As described above and in Attachment B, this application seeks to search and seize records that might be found at 21 School House Rd, Greenfield, NH, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure and search of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

26. I submit that if a computer or storage medium, including desktop computer, laptop computer, and wireless or mobile telephone, is found at 21 School House Rd, there is probable cause to believe those records will be stored on that computer or storage medium for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by

an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

27. As set forth above, probable cause exists to believe that ARSENAULT is using electronic devices to buy and sell binary exploding target materials similar to Tannerite, and marketed as such, as well as other items similar to those recovered from the damaged Jeep. Based up on my knowledge and experience, and the experience of other law enforcement officers with whom I have discussions, I know that individuals also typically conduct internet searches and online research to learn how to construct IEDs and other destructive devices. Furthermore, ARSENAULT claimed to others to have researched explosive materials online at explodingtargets.com as well as other previously referenced websites.

28. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the

purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer 21 School House Rd because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it and when, it is sometimes necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

24. Based on my training and experience I know that much of the media referenced above, which may contain contraband, fruits and evidence of crime, is by its very nature portable. This includes as example but is not limited to extremely compact storage devices such as thumb drives, laptop computers, and smart phones. In my training and experience, I know it is not uncommon for individuals to keep such media in multiple locations within their premises, including in outbuildings and motor vehicles.

25. Searching storage media for the evidence described in the attachment may require a range of data analysis techniques. In most cases, a thorough search for information stored in storage media often requires agents to seize most or all electronic storage media and later review the media consistent with the warrant. In lieu of seizure, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic

picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. **The nature of evidence**. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly search storage media to obtain evidence, including evidence that is not neatly organized into files or documents. Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a warrant, a search of this premises for the things described in this warrant will likely require a search among the data stored in storage media for the things (including electronic data) called for by this warrant. Additionally, it is possible that files have been deleted or edited, but that remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use more thorough techniques.

b. **The volume of evidence**. Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files is evidence or instrumentalities of a crime. This sorting process can take weeks or months, depending on the

volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

c. **Technical requirements**. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

d. **Variety of forms of electronic media**. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

26. Based on the foregoing, and consistent with Rule 41(e)(2)(B), when officers executing the warrant conclude that it would be impractical to review the hardware, media, or peripherals on-site, the warrant I am applying for would permit officers either to seize or to image-copy those items that reasonably appear to contain some or all of the evidence described in the warrant, and then later review the seized items or image copies consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

29. Based on the aforementioned related facts, I submit that this Affidavit supports probable cause for a warrant to search the Premises located at 21 School House Rd, Greenfield,

NH 03047 as described in Attachment A and any computer and electronic media located therein, and seize the items described in Attachment B.

30. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

REQUEST FOR SEALING

31. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

/s/ Shayne Tongbua
Shayne Tongbua
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on February 6, 2019 at Concord, New Hampshire.

/s/ Andrea K. Johnstone
Honorable Andrea K. Johnstone
United States Magistrate Judge
District of New Hampshire

ATTACHMENT A

Property to Be Searched

I. Residence

The property to be searched is 21 School House Rd, Greenfield, NH 03047, identified as a single family residence occupied by Alexander ARSENAULT. The primary structure is a two-story house, which has light gray siding with a dark roof and white window shutters. The residence is accessed by a white exterior door accessible from the driveway side of the house. The driveway is accessible from School House Rd and is the last driveway before the end of the road which is impassible due to a damaged bridge.

Also to be searched on the property is a detached garage located adjacent to the main dwelling, accessible from the driveway, as well as a utility shed located immediately behind the house. Photographs of the residence are below:

ATTACHMENT B

Particular Items to be Seized

All items that constitute evidence and instrumentalities of violations of 18 U.S.C. § 33 and 26 U.S.C. § 5861(c), (f), involving Alexander ARSENAULT, or information pertaining to the following matters:

1) Records, information, and items relating to violations of the statutes described above including:
   a. Bills, mail, or addressed correspondence relating to the occupancy or ownership of 21 School House Rd, Greenfield, NH 03047;
   b. Documents, photographs, videos, and messages relating to the sale, purchase, acquisition, possession or utilization of explosive materials, precursor substances, or related accessories by ARSENAULT.
   c. Evidence indicating how and when explosive materials were acquired or used, to determine the chronological and geographic context of use and events relating to the crimes under investigation and to the owner;
   d. Sales receipts, product registration documentation, bills for internet access, and handwritten notes relating to the ownership of computer equipment in the above residence;
2) Explosive materials, precursor chemicals or substances, and related accessories.
3) Mail or packages potentially containing chemicals, materials or equipment used as a means to commit the violations described above.
4) Any computer, mobile telephone, or electronic media that were or may have been used as a means to commit the offenses described on the warrant.

5) computer hard drive, or other physical object upon which electronic data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

   a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

   b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

   c. evidence of the lack of such malicious software;

   d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

   e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

   f. evidence of the times the COMPUTER was used;

   g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

   h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

   i. contextual information necessary to understand the evidence described in this attachment.

6) Records and things evidencing the use of the Internet, including:

   a. routers, modems, and network equipment used to connect computers to the Internet;

   b. records of Internet Protocol addresses used;

   c. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

As used above, the term “COMPUTER” includes but is not limited to any and all computer equipment, including any electronic devices that are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. These devices include but are not limited to any data-processing hardware (such as central processing units, memory typewriters, mobile “smart” telephones, tablets, and self-contained “laptop” or “notebook” computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, thumb drives, flash drives, Micro SD cards, SD cards, CDs, DVDs, tape drives and tapes, optical storage devices, zip drives and zip disk media, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, fax machines, digital cameras, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as modems, routers, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks).